Trasferimento dei dati all’estero: quali soluzioni?

Introduzione

Come sarà ormai noto a tutti, qualunque trasferimento di dati personali verso un paese terzo o un’organizzazione internazionale può avvenire esclusivamente alle condizioni descritte al capo V del Regolamento generale sulla protezione dei dati, che hanno il fine di assicurare che il livello di protezione delle persone fisiche garantito dal GDPR non sia pregiudicato (cfr at. 44 RGPD).

Nel capo in commento vengono indicate le misure di salvaguardia che possono consentire un trasferimento lecito “extra UE” (o meglio, al di fuori dallo Spazio Economico Europeo), e tra queste vi sono le decisioni di adeguatezza (art. 45 GDPR), che vengono prese dalla Commissione Europea all’esito di peculiari valutazioni, e, in mancanza di decisioni di adeguatezza, altri sistemi meno immediati, come le clausole contrattuali standard – o clausole contrattuali tipo (articolo 46).

Anche le clausole contrattuali standard, in realtà, in prima battuta sono adottate con decisione della Commissione Europea, che ne determina forma e sostanza. Le imprese che per effettuare trasferimenti extra SEE decidono di ricorrere alle clausole contrattuali standard devono necessariamente usare il modello corrispondente alle loro necessità (le clausole variano a seconda che il trasferimento verso l’importatore di dati debba avvenire tra titolare e responsabile del trattamento, o tra titolari).

Le multinazionali possono avvalersi di un ulteriore strumento, le norme vincolanti d’impresa, che hanno però una procedura

relativamente lunga e complessa. Non risultano ancora implementati gli ulteriori sistemi previsti dall'articolo in commento (certificazioni e codici di condotta)

Gli interventi della Corte di Giustizia

Quando la Corte di Giustizia con la sentenza nota come Schrems I (dal nome dell'attivista che le diede impulso) travolse il Safe Harbor – una decisione di adeguatezza che presidiava la maggior parte dei trasferimenti di dati personali verso gli USA- buona parte dei maggiori provider e buona parte delle imprese che operavano in più Paesi, decisero di adottare come strumento di trasferimento le clausole contrattuali standard (molti provider, ad esempio, le resero accessibili nelle aree riservate, in modo che i titolari del trattamento potessero aderirle).

Con l'avvento del Privacy Shield- una decisione di adeguatezza volta a colmare il vuoto lasciato dal Safe Harbor- molti titolari decisero di mantenere il doppio binario di trasferimento (nulla vieta, infatti, di poggiare il trattamento all'estero su due diverse misure di salvaguardia) così da non restare scoperti nel caso in cui anche il Privacy Shield per qualche ragione fosse venuto meno.

Cosa che infatti è puntualmente avvenuta, con la sentenza Schrems II: questo primo effetto, ampiamente atteso, non ha causato un terremoto, perchè molti si aspettavano che il Privacy Shield, un ponteggio allestito in fretta e furia, esposto a continua erosione sia per le critiche mosse dal Comitato dei Garanti (EDPB) sia per quelle di esperti e attivisti, crollasse miseramente da un momento all'altro.

Molti però confidavano che sarebbe rimasto in piedi l'altro strumento di transito, cioè le clausole contrattuali standard: la sentenza Schrems II, invece, ha minato completamente anche questo terreno, trasformando in via impervia quello che prima appariva come un corridoio di transito collaudato e sicuro.

Come ha fatto la Corte di Giustizia ad ottenere un tale effetto?

Nella sentenza Schrems II la Corte di Giustizia ha invalidato direttamente il Privacy Shield, ma non ha direttamente invalidato le clausole contrattuali standard.

La Corte di Giustizia, però, ha aggiunto alcuni elementi molto importanti:

ha dichiarato, infatti, che in caso di trasferimenti verso un paese terzo occorre garantire agli interessati un livello di protezione **sostanzialmente equivalente** a quello garantito all'interno dell'Unione dal GDPR, letto alla luce della Carta dei diritti fondamentali dell'Unione europea.

Chi intende trasferire dati con le clausole contrattuali standard, pertanto, dovrà valutare non solo il contenuto delle clausole contrattuali standard medesime, ma anche "*per quel che riguarda un eventuale accesso delle autorità pubbliche di tale paese terzo ai dati personali così trasferiti, gli elementi rilevanti del sistema giuridico di quest'ultimo* (…)".

Per quanto riguarda la valutazione della normativa statunitense, la Corte di giustizia offre parametri piuttosto precisi circa i trattamenti che possono essere effettuati a fini di sicurezza pubblica, di difesa e sicurezza dello Stato. Sono gli stessi parametri che hanno condotto la Corte alla invalidazione del privacy shield. Difficilmente potrà giungersi a diverse conclusioni ove analoghe valutazioni venissero applicate a diversi sistemi di trasferimento dei dati "verso" gli USA (il virgolettato si impone, perché, come vedremo, non sempre è necessario che i dati siano fisicamente allocati negli USA -o in altro Paese Terzo).

Se non si riesce a garantire il livello di protezione ***sostanzialmente equivalente*** a quello garantito all'interno dell'Unione Europea dal GDPR, il Titolare dovrà interrompere il trasferimento, o, in mancanza, dovrà farlo L'Autorità di

protezione dei dati nazionale.

La Sentenza della Corte di Giustizia pone principi che non valgono solo per le clausole contrattuali standard, ma anche per le norme vincolanti d'impresa, compromettendo l'applicazione dell'intero articolo 46 del Regolamento.

L'intervento dell'EDPB

E' ovvio che un tema importante come quello sollevato dalla sentenza Schrems II non poteva cadere nel vuoto, e gli interventi degli organismi chiamati a coordinare l'applicazione del Regolamento generale sulla protezione dei dati nei vari Paesi Europei non si sono fatti attendere.

Il primo intervento del Comitato Europeo per la protezione dei dati (l'organo che raccoglie le Autorità per la protezione dei dati nazionali più il Garante europeo, di seguito anche EDPB dall'acronimo con cui è conosciuto universalmente) si è avuto con le FAQ relative alla sentenza Schrems II.

Il Comitato ha chiarito che, "*in generale, per i paesi terzi, la soglia fissata dalla Corte si applica anche a tutte le garanzie adeguate di cui all'articolo 46 del RGPD, utilizzate per il trasferimento dei dati dal SEE a qualsiasi paese terzo. La normativa statunitense richiamata dalla Corte [l'articolo 702 del Foreign Intelligence Surveillance Act (FISA) e l'Executive Order (EO) 12333] si applica a qualsiasi trasferimento verso gli Stati Uniti eseguito con mezzi elettronici che rientri nell'ambito di applicazione della suddetta normativa, a prescindere dallo strumento utilizzato per il trasferimento*".

Qualunque strumento si stia utilizzando, pertanto, occorrerà effettuare una valutazione della normativa del Paese Terzo, considerando anche le norme che regolano gli accessi ai dati per fini di sicurezza pubblica, di difesa e sicurezza dello Stato.

Occorrerà quindi valutare il livello di garanzia apportato dalle clausole contrattuali standard, alla luce della stima operata sulla normativa del Paese terzo.

Occorrerà poi individuare misure tecniche e organizzative (ma anche contrattuali) supplementari, che possano garantire un livello di protezione sostanzialmente equivalente a quello offerto dal GDPR nello Spazio Economico Europeo.

Come precisa L'EDPB "*La possibilità di trasferire dati personali sulla base delle clausole contrattuali tipo dipenderà dall'esito della valutazione condotta; tenendo conto delle circostanze dei trasferimenti e delle misure supplementari eventualmente attuabili.*

Le misure supplementari unitamente alle clausole contrattuali tipo, previa analisi caso per caso delle circostanze del trasferimento, dovrebbero assicurare che la normativa statunitense non interferisca con il livello di protezione adeguato dalle stesse garantito.

Qualora si giunga alla conclusione che, tenuto conto delle circostanze del trasferimento e delle possibili misure supplementari, non sarebbero assicurate garanzie adeguate, vi è l'obbligo di sospendere o cessare il trasferimento dei dati personali. Se si intende tuttavia proseguire col trasferimento dei dati malgrado la suddetta conclusione, è obbligatorio informarne l'autorità di controllo competente".

La soluzione suggerita dall'EDPB passo passo

Al fine di chiarire ulteriormente gli adempimenti che dovrebbero condurre il Titolare nelle sue valutazioni, il Comitato Europeo per la Protezione dei dati – ha pubblicato innanzi tutto le "*Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*

Adopted on 10 November 2020" che si pongono l'obiettivo di offrire un catalogo dei parametri da rispettare nella valutazione della normativa del Paese terzo in materia di sicurezza nazionale qualora le misure di sorveglianza del Paese terzo consentano l'accesso ai dati personali ad Autorità pubbliche, in modo da comprendere se tali interferenze possano essere giustificabili o meno. Esse però non esauriscono di per sé la valutazione che il Titolare è chiamato a compiere.

Quindi al fine di fornire uno strumento più concreto e ampio sono state pubblicate anche le "*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*" **che resteranno in consultazione pubblica fino al 21 dicembre 2020.**

Queste ultime si pongono l'ambizioso obiettivo di coadiuvare coloro che trasferiscano dati all'estero nella complessa valutazione che sono chiamati ad operare sulla normativa del Paese terzo e nell'individuazione delle misure supplementari che si rendessero necessarie. Le raccomandazioni si compongono di una serie di *step* che coloro che esportano dati personali dovrebbero seguire, suggerimenti sulle possibili fonti di informazioni e alcuni esempi di misure supplementari che potrebbero essere adottate.

I primi step

Il primo passo suggerito dal Comitato, condivisibile, è come sempre quello di conoscere quello che si fa, quindi: mappare i trasferimenti. Il CEPD riconosce che una simile mappatura potrebbe non essere una operazione facile: essa tuttavia appare imprescindibile per garantire un livello di protezione essenzialmente equivalente a quello offerto dal GDPR nel SEE.

La mappatura consentirà di valutare se i trasferimenti siano adeguati, pertinenti e limitati a quanto strettamente necessario in relazione alla finalità perseguita.

Il secondo step sarà quello di verificare lo strumento di trasferimento, se, cioè si stia utilizzando una decisione di adeguatezza o se invece ci si fondi su uno degli altri meccanismi previsti dall'articolo 46 GDPR.

Se i trasferimenti sono poggiati esclusivamente su decisioni di adeguatezza, allora la valutazione potrà arrestarsi qui (almeno fino a quando permarrà la decisione di adeguatezza…)

A questo punto, per meglio comprendere la portata della mappatura, chi scrive farà alcune considerazioni, partendo da una osservazione lapalissiana, e cioè che la definizione di dato personale è amplissima: gli indirizzi IP sono dati personali, per esempio. In linea generale, i dati pseudonimizzati sono dati personali. E non solo: quando parliamo di trasferimento extra UE, dimentichiamo spesso di considerare che anche l'accesso da remoto potrebbe essere un trasferimento: come precisa il CEPD alla nota 22: "*Please note that remote access by an entity from a third country to data located in the EEA is also considered a transfer*": insomma se è possibile per un governo straniero accedere a dati allocati nello Spazio Economico Europeo (lo stesso ambito di applicazione del GDPR), allora si avrà un trasferimento di dati personali per cui sarà necessario seguire tutti gli Step indicati.

Non importa pertanto che i dati risiedano fisicamente su server che si trovano nello Spazio Economico Europeo: quando l'impresa che li tratta è sotto la giurisdizione di un Paese terzo non adeguato ed è previsto dalle norme del medesimo Paese terzo che le sue autorità possano accedere ai dati sul server in UE, allora siamo in presenza di un trasferimento di dati per cui è necessario procedere alla valutazione e alla applicazione, oltre che degli strumenti previsti dall'articolo 46, anche delle misure supplementari.

Tanto chiarito sia in ordine alla definizione di dato personale, sia in ordine alla estensione della nozione di

“trasferimento”, pensiamo a quanti servizi possono essere interessati dal trasferimento dei dati all’estero, seppure i dati siano trattati in Europa: social network, servizi email, gestionali, servizi di condivisione o hosting di documenti, servizi di sicurezza dei siti web che trattano esclusivamente indirizzi IP, strumenti di analisi, quasi tutti i servizi di marketing, per citare i più diffusi.

Il Comitato europeo per la protezione dei dati ha anche ribadito che in assenza di una decisione di adeguatezza, occorrerà che il trasferimento sia assistito da uno degli strumenti previsti dall’articolo 46 GDPR, se i trasferimenti sono regolari e ripetitivi, **e solo in caso di trasferimento di dati personali occasionali e non ripetitivi**, si potrebbero quindi utilizzare gli strumenti previsti invece dall’articolo 49 GDPR, se ne sussistono tutte le condizioni. Su questo punto sarebbero auspicabili maggiori chiarimenti, dato che diversi esperti prefigurano un ricorso massivo ai mezzi previsti dall’articolo 49 GDPR in conseguenza della paralisi in cui versa, almeno per alcune tipologie di trattamento, l’articolo 46 del Regolamento, impostazione che al momento non parrebbe però avallata dal laconico rinvio operato dal Comitato alle proprie pregresse posizioni (cfr Linee guida 2/2018 sulle deroghe di cui all’articolo 49 del regolamento 2016/679).

Il terzo step consiste nello stimare se vi siano elementi nella normativa o nella prassi del Paese terzo che possano impattare sulla effettiva protezione della salvaguardia adottata per il trasferimento, nel contesto dello specifico trasferimento effettuato.

La valutazione deve prima indagare la normativa del Paese terzo (che sia rilevante rispetto al trasferimento effettuato e la misura di trasferimento adottata ai sensi dell’articolo 46) che potrebbe compromettere il livello di protezione, poi la prassi.

La valutazione sulla normativa va operata alla stregua delle

“Recommendations 02/2020 on the European Essential Guarantees for surveillance measures Adopted on 10 November 2020”. Occorrerà prestare particolare attenzione soprattutto qualora le norme che regolano l’accesso ai dati da parte di Autorità pubbliche del Paese Terzo non siano chiare o disponibili al pubblico.

Anche in assenza di norme di tal fatta, prima di procedere al trattamento occorrerà valutare altri fattori, definiti dal CEPD “rilevanti e obiettivi” e non basarsi su fattori soggettivi come la probabilità che le Autorità del Paese terzo accedano ai dati in maniera non conforme agli standard dell’Unione Europea.

Chi scrive avrebbe voluto riferire quanto riportato nelle raccomandazioni senza annotazioni, ma qui un rilievo si impone. Dato che il GDPR è un sistema basato sulla valutazione del rischio, ci si aspetta che l’ulteriore valutazione che si viene chiamati a compiere dal CEPD si basi su criteri probabilistici, come è di regola nel risk assessment. Invece no: la valutazione della probabilità che i dati che ci prefiggiamo di trasferire costituiscano l’obiettivo di un organismo governativo che effettua sorveglianza per ragioni di sicurezza nazionale, viene liquidato come parametro meramente soggettivo. Occorrerà quindi mettere in piedi una procedura di due diligence documentata, cercando informazioni da altre fonti come: precedenti, risorse organizzative e tecniche dello Stato terzo, ecc. Chi scrive vuole richiamare due punti importanti per comprendere pienamente la portata di questa valutazione. Nel nostro Paese abbiamo una costellazione di PMI e professionisti che trasferiscono dati in Paesi extra SEE, che non possono effettuare l’assessment richiesto dall’EDPB: non ne hanno i mezzi. Peraltro, quando parliamo di Paesi terzi non ci riferiamo ai soli Stati Uniti, ma a qualunque Paese non abbia ricevuto una decisione di adeguatezza: pensiamo cosa significhi effettuare una simile indagine su un Paese come la Cina, ove anche la lingua costituirà un ostacolo non banale.

Vedremo se questa impostazione verrà confermata dopo la consultazione pubblica, ma certamente il criterio della probabilità dell'accesso da parte del governo straniero potrebbe rivelarsi cruciale per gli operatori e chi scrive si auspica sul punto una maggiore apertura.

Gli step finali

Il quarto step in apparenza restituisce qualche blanda speranza: identificare le misure

supplementari per innalzare il livello di protezione di dati personali agli standard europei.

Questo step, precisa il Comitato Europeo per la protezione dei dati, è necessario solo qualora, all'esito dell'indagine, si evidenziasse che la normativa del Paese Terzo, impatti sulla effettività delle misure di salvaguardia ex art. 46 GDPR. Ma appare difficile a chi scrive immaginare che l'esito della complessa indagine condotta sia diverso. Come potrebbero strumenti di natura pattizia arginare il potere dello Stato in materia di sicurezza nazionale?

Ci torneremo tra poco.

Il quinto step esprime la necessità di adottare formalmente le misure supplementari individuate.

Il sesto prevede un meccanismo di revisione periodica, che imporrà quindi una nuova analisi della normativa (e non solo, come si è visto sopra) del Paese terzo.

Tornando quindi al quarto step, c'è un intero allegato ("annex 2") che contiene una lista esemplificativa e non esaustiva di misure che possono essere adottate.

L'EDPB precisa che talune potrebbero essere efficaci in alcuni Paesi e non in altri.

Colui che decide di trasferire i dati, pertanto, resterà

l'unico responsabile della valutazione operata e della efficacia delle misure supplementari adottate, nel contesto del trattamento effettuato, alla luce della normativa (e delle prassi!) del Paese terzo, degli strumenti di salvaguardia adottati ai sensi dell'articolo 46, e delle misure supplementari cui decidesse di ricorrere.

Il tutto dovrà essere documentato e si potrebbe anche rendere necessario combinare più misure supplementari. Ove comunque all'esito del "*personal data transfer impact assessment*" non si riuscisse ad ottenere un livello di protezione sostanzialmente equivalente a quello offerto dall'UE, il trasferimento dovrà essere interrotto, sospeso o evitato, per non compromettere il livello di protezione dei dati personali dell'interessato.

In ordine al rapporto tra misure contrattuali, organizzative e tecniche, le prime (cioè le misure organizzative e contrattuali) appaiono il più delle volte strettamente connesse con le misure tecniche alle quali forniscono una sponda, ma difficilmente le misure contrattuali e organizzative potranno essere "autoportanti".

Quali misure supplementari preferire? La lettura degli scenari immaginati dal CEPD offre molti spunti. Uno strumento aggiuntivo di protezione dei dati suggerito da più parti già alla prima lettura della sentenza Schrems II è la crittografia. Ed in effetti essa viene indicata più volte tra le misure tecniche.

Non si creda tuttavia che sia sufficiente applicare la crittografia all'esito della complessa valutazione operata per superare gli stretti limiti posti dall'EDPB: come detto, vi è una lunga serie di esempi che vengono portati a corredo delle considerazioni sopra brevemente riassunte, e appaiono notevoli gli scenari indicati sub "Scenarios in which *no effective* measures could be found" e in particolare quelli indicati al punto 88 "*Use Case 6: Transfer to cloud services providers or*

other processors which require access to data in the clear" e 90 "*Use Case 7: Remote access to data for business purposes*": si tratta di configurazioni che riguardano la maggior parte dei cloud saas (e non solo), che appaiono, *prima facie*, impossibili da regolarizzare.

Infine anche le misure contrattuali suggerite appaiono foriere di gravami e costi per l'importatore di dati, che può trovarsi a dover fornire informazioni che esulano dalla sua area di attività, come ad esempio informazioni sulla legislazione, o addirittura ad assumersi l'obbligo, in determinate condizioni, di opporsi alle richieste governative: si tratta di pattuizioni non banali, pertanto, che potrebbero avere serie ripercussioni sui costi del servizio soprattutto ove i servizi siano offerti da aziende che non hanno le spalle larghe dei giganti della Silicon Valley.

Le clausole contrattuali standard

In questo contesto piuttosto complesso si inscrive l'intervento della Commissione Europea, che ha pubblicato la bozza dei nuovi testi delle clausole contrattuali standard, anch'essi sottoposti a consultazione pubblica.

La prima nota positiva è che finalmente vengono introdotti i trasferimenti da responsabile a subresponsabile ("processor to processor"), che ancora non avevano un testo *ad hoc.*

La seconda annotazione è che paiono riferirsi solo a parte dei trasferimenti presi in considerazione dall'EDPB: e anche le misure indicate non appaiono perfettamente allineate a quelle suggerite dal Comitato.

Non è questa la sede per una disamina della bozza delle clausole contrattuali standard, che meriterebbe uno spazio a sé, tuttavia non si può tralasciare un dato importante, che riguarda l'ambito di applicazione: nella bozza "COMMISSION IMPLEMENTING DECISION (EU) …/… of XXX on standard contractual

clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council" (Ref. Ares (2020)6654686 – 12/11/2020) all'articolo 1 si legge: "*The standard contractual clauses set out in the Annex are considered to provide appropriate safeguards within the meaning of Article 46(1) and (2)(c) of Regulation (EU) 2016/679 for the transfer of personal data from a controller or processor subject to Regulation (EU) 2016/679 (data exporter) to a controller or (sub-) processor not subject to Regulation (EU) 2016/679 (data importer).*"

Significa che le clausole contrattuali standard, qualunque esse siano, si applicheranno **solo ove l'esportatore di dati personali sia soggetto alla applicazione del Regolamento, mentre l'importatore non lo sia**.

L'ambito di applicazione del RGPD prescinde dal criterio prettamente geografico della allocazione dei dati o della sede (o stabilimento dell'impresa), come è noto, e il GDPR si applica anche "al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento **che non è stabilito nell'Unione,** quando le attività di trattamento riguardano:

1. a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
2. b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione."Pertanto l'ambito di applicazione delle clausole contrattuali standard appare agganciato all'ambito del trattamento delineato dall'articolo 3 del Regolamento generale sulla protezione dei dati e non appare coincidere con quello tratteggiato dall'EDPB, che invece non chiarisce il rapporto tra l'articolo 3 e il

capo V del Regolamento generale sulla protezione dei dati, e come abbiamo visto sopra, richiama criteri molto ampi per individuare i trasferimenti all'estero (che però sono in linea con la sentenza Schrems II). Ciò significa che potremmo avere dei trasferimenti extra SEE non coperti dalle clausole contrattuali standard.

La mancanza della definizione del trattamento dei dati all'estero nel testo del Regolamento si fa sentire in tutta la sua potenza. Vedremo se all'esito della consultazione pubblica i testi troveranno una miglior coordinazione.

Quali soluzioni per i trasferimenti extra UE?

Dalla lettura della casistica individuata dall'EDPB si evince facilmente che non esiste una soluzione unica, ma molteplici soluzioni a seconda delle diverse tipologie di trattamento.

Un primo dato che possiamo trarre è che la soluzione di cercare più meccanismi di trasferimento per garantire un trattamento contro cambi di rotta repentini, non è più praticabile per le piccole imprese (ad esempio: appoggiarsi al doppio binario costituito da decisione di adeguatezza e clausole contrattuali standard). O meglio, è praticabile al costo di dover effettuare una valutazione di impatto sul trasferimento: abbiamo visto grazie a Schrems quanto possano essere precarie le decisioni di adeguatezza, ma non è detto che riusciremo ancora ad appoggiare i trasferimenti coperti da decisioni di adeguatezza anche alle clausole contrattuali standard, almeno fino a quando non avremo il nuovo testo (e sempre che sia possibile utilizzarle in relazione al concreto trasferimento posto in essere).

La maggiori problematiche, al momento, sono rinvenibili nel fatto che la sentenza Schrems II produce già ora i suoi effetti e come precisa l'EDPB il periodo di consultazione pubblica non va interpretato come un periodo di grazia.

A diverse conclusioni non giunge la Commissione Europea, che ritiene che per un periodo di un anno a far data dalla entrata in vigore della nuova decisione sulle SCC, i trasferimenti potranno basarsi sulle pregresse clausole contrattuali aggiornate con le necessarie misure di salvaguardia.

Cosa bisogna fare dunque? Non vi è molta scelta, occorrerà procedere alla mappatura dei trasferimenti, alla valutazione di impatto del trasferimento con analisi della normativa e delle prassi del Paese terzo (con tutte le difficoltà che ciò può comportare) ed infine individuare le misure supplementari.

Non è scontato che l'esito dell'esame sia favorevole al trasferimento, anzi: alcuni dei servizi più utilizzati potrebbero non trovare appigli in adeguate misure tecniche, quanto alle misure contrattuali occorre realisticamente tenere conto dello squilibrio di forza contrattuale tra le PMI e i maggiori provider di servizi, per cui, in assenza di iniziative che partano dai fornitori, difficilmente si troveranno soluzioni praticabili.

L'elefante nella stanza

In effetti a parere (non solo) di chi scrive è possibile che gli effetti della sentenza Schrems II abbiano finito col disattivare, in un certo senso, buona parte degli strumenti di trasferimento dei dati più utilizzati dalle imprese e, addirittura, finiscano col paralizzare completamente la possibilità di effettuare alcuni tipi di trasferimenti.

Gli effetti sono tali perché nonostante gli sforzi che possiamo fare, come è già stato autorevolmente rilevato, l'unica vera soluzione ha una portata internazionale: se il problema è il conflitto tra due o più ordinamenti non saranno né i privati né gli organismi di un solo ordinamento a poterlo risolvere.

La necessità impellente di un accordo internazionale è

l’elefante nella stanza, ed è impossibile giunti a questo punto continuare ad ignorarlo: Europa ed USA, per restare ai contendenti più noti, giocano la partita spingendo quanto più possibile le loro norme oltre i confini territoriali: in questo modo però arriviamo al paradosso per cui un’impresa, soggetta alla giurisdizione di un Paese non adeguato, che tratta dati su suolo europeo (nel SEE!) non offre sufficienti garanzie per i parametri fissati dalla stessa UE, anche ove le si applichi il GDPR (ai sensi dell’articolo 3 del GDPR medesimo). E’ evidente che in un quadro simile (impresa che applica il GDPR, si trova in UE, ma non offre garanzie sufficienti perché accessibile da parte di Agenzie Governative del Paese terzo) il problema travalica ogni valutazione di impatto che si possa compiere (per non parlare dei casi che riguardano i gruppi di imprese) ed è ormai del pari evidente che il problema non potrà essere nascosto sotto gli arabeschi di un tappeto di adempimenti più o meno burocratizzati, buoni nella migliore delle ipotesi a guadagnare tempo prima della prossima sentenza tranciante della Corte di Giustizia, nella peggiore sino al prossimo *whistleblower* che ne palesi l’inconsistenza. In assenza di un accordo internazionale solido come una casa di mattoni, continueremo a proteggere i trasferimenti di dati personali con capanne di paglia e legno, come i porcellini della nota fiaba, ben sapendo che saranno soffiate via dal primo lupo che passa.

Riferimenti

1. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (Testo rilevante ai fini del SEE) LINK: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016R0679

2. Sentenza Schrems I – SENTENZA DELLA CORTE (Grande Sezione) 6 ottobre 2015 Nella causa C-362/14 http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=388
3. Sentenza Schrems II SENTENZA DELLA CORTE (Grande Sezione) 16 luglio 2020 Nella causa C-311/18 http://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=IT
4. Domande piu` frequenti in merito alla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 – Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems https://edpb.europa.eu/our-work-tools/our-documents/ohrajn/frequently-asked-questions-judgment-court-justice-european-union_en
5. Recommendations 02/2020 on the European Essential Guarantees for surveillance measures https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en
6. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data – version for public consultation https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en
7. Tene, Omer (Vice President, Chief Knowledge Officer at IAPP – International Association of Privacy Professionals): "Quick Reaction to EDPB Schrems II Guidance" https://www.linkedin.com/pulse/quick-reaction-edpb-schrems-ii-guidance-omer-tene/
8. Data protection – standard contractual clauses for transferring personal data to non-EU countries (implementing act)

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries
9. Scorza, Guido (Autorità Garante Privacy) “Trasferimento dati extra-Ue, Scorza (Garante Privacy): Abbiamo un problema, anzi tre” https://www.agendadigitale.eu/sicurezza/privacy/trasferimento-dati-extra-ue-abbiamo-un-problema-anzi-tre-e-non-riguarda-solo-gli-usa/

Articolo a cura di **Cristina Vicarelli**

https://www.ictsecuritymagazine.com/articoli/trasferimento-dei-dati-allestero-quali-soluzioni/